Google

ssdp upnp Search Advanced Search Preferences

New! View and manage your web history

Web

Results **31** - **40** of about **120,000** for **ssdp upnp**. (**0.10** seconds)

eEye Digital Security - Research
UPNP consists of multiple protocols, one of which being the Simple Service Discovery Protocol (**SSDP**). When a **UPNP** enabled device is installed on a network, ...
www.eeye.com/html/Research/Advisories/AD20011220.html - 25k - Cached - Similar pages

Hanno Meyer-Thurow - gcj-4.2-20060819 and azureus-2.5.0.0
UPnPException: Failed to initialise **SSDP** at com.aelitis.net.**upnp**.impl.**ssdp**.
SSDPCore.<init>(SSDPCore.java:124) at com.aelitis.net.**upnp**.impl.**ssdp**.SSDPCore. ...
gcc.gnu.org/ml/java/2006-08/msg00082.html - 8k - Cached - Similar pages

ÔÃ²¡ ÿÿ CÛ¦A²a G G â !@ à †žÆ E 9 @ @ ´üÀ¨ fÀ¨ 5 %ò;÷M ddraig fire ...
... Cache-Control:max-age=60 Location:http://192.168.2.1/igd.xml NT:**upnp**:rootdevice
NTS:**ssdp**:alive Server:SMC2804WBRP-G/v1.00 **UPnP**/1.0 **UPnP**-Device-Host/1.0 ...
www.cs.sfu.ca/CourseCentral/471/jregan/assignments/ass3/dnsetherealcapture - 12k -
Cached - Similar pages

Upnp2sClientControlPoint (Trace URC SDK Documentation)
public void deviceSearchResponseReceived(org.cybergarage.**upnp**.**ssdp**.SSDPPacket packet). Specified by:: deviceSearchResponseReceived in interface ...
myurc.org/tools/UrcSdk/doc/edu/wisc/
trace/urcsdk/client/**upnp**2s/**Upnp**2sClientControlPoint.html - 30k - Cached - Similar pages

NEOHAPSIS - Peace of Mind Through Integrity and Insight
UPNP consists of multiple protocols, one of which being the Simple Service Discovery Protocol (**SSDP**). When a **UPNP** enabled device is installed on a ...
www.security-express.com/archives/vulnwatch/2001-q4/0075.html - 16k -
Cached - Similar pages

Missing tray icons
Methods/workarounds: Log off and Log back on, password protect your account or disable **SSDP** and **uPNP** Services. Disable **SSDP** and **uPNP** Services (Line 156) ...
www.tomshardware.com/forum/56875-45-missing-tray-icons - 51k - Cached - Similar pages

Software architecture for out-of-band discovery in **UPnP** - Patent ...
2 is representation of a **UPnP** software stack with **SSDP** PI as an out-of-band ... The payload of this message is the same as for a standard **UPnP SSDP** message: ...
www.freepatentsonline.com/20060095574.html - 34k - Cached - Similar pages

Problems with DGL-4300 - dslreports.com
UPnP::**SSDP**: ignoring loopback address /0:0:0:0:0:0:0:1 **UPnP**::**SSDP**: ignoring IPv6 ...
UPnP::**SSDP**: ignoring IPv6 address /xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx ...
www.dslreports.com/forum/remark,14394681 - Similar pages

Help with **SSDP** service - Windows Forum
The only dependent service for the **SSDP** discovery service is HTTP. I do not see an HTTP service ony my services list, just HTTP SSL. I have **UPnP** installed, ...
www.thescripts.com/forum/thread543640.html - 33k - Cached - Similar pages

How does Zeroconf compare with Viiv/DLNA/DHWG/**UPnP**?
For example, many printers claim to implement **UPnP**, and indeed examining the network with a packet sniffer will show that the printer is sending **UPnP SSDP** ...
www.zeroconf.org/ZeroconfAnd**UPnP**.html - 18k - Cached - Similar pages

Previous 1 2 3 **4** 5 6 7 8 9 10 11 12 13 **Next**

ssdp upnp Search

Search within results | Language Tools | Search Tips

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	347363	kim.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:23
S2	1	doheon.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:23
S3	1	S1 and S2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:23
S4	234644	samsung.as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:28
S5	6535	(709/224).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/08/24 10:29
S6	65822	((search$4 discover$4) near4 (device node service))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:30
S7	1033	S6 and upnp	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:30

EAST Search History

S8	2020	upnp	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:30
S10	51	"control point server"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:31
S11	9	S10 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:31
S9	47	S5 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:58
S12	107124	((search$4 discover$4) same (description))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:58
S13	6929	S6 same (description describe)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:59
S14	540	S12 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:59

EAST Search History

S15	193	S14 and (@AD<"20030214" @RLAD<"20030214")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 10:59
S16	71	S8 and ((multiple many) near3 (response))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:39
S17	175	S8 and ((second) near3 (response))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:39
S18	138	S8 and ((second) near2 (response))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:39
S19	52	S8 and ((second) near (response))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:49
S20	11	S8 and ((second) adj (response))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:50
S21	12	S8 and ((first) adj (response))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:51

EAST Search History

S23	2	S22 and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:51
S24	478	S22 and (@AD<"20030214" @RLAD<"20030214")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:53
S25	49	S24 and "709".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:53
S22	839	first same second same response same ("not" ignore)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:54
S26	23	(first near2 response) same (second near2 response) same ("not" ignore)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:58
S27	75	(first near2 message) same (second near2 message) same ("not" ignore)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 12:59
S28	88	(first near2 message) same (second near2 message) and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 13:04

EAST Search History

S29	2	(ignor$4 near3 (second subsequent other additional)) and S8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 13:11
S30	624	(ignor$4 near3 (second subsequent other additional)) with (response answer message)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 13:25
S31	209	S8 same directory	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 13:26
S32	2	S8 and (period$5 with check$4 with status)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 17:00
S33	71	S8 and (check$4 near5 status)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 17:01
S34	51	S8 and ((check$4 near5 status) same device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/24 18:05
S35	2	("7143143").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/08/24 18:06

UPNP - Multiple Remote Windows XP/ME/98 Vulnerabilities

Release Date:
December 20, 2001

Severity:
High

Vendor:
Microsoft

Systems Affected:
Microsoft Windows XP (All default systems)
Microsoft Windows 98 (Certain configurations)
Microsoft Windows 98SE (Certain configurations)
Microsoft Windows ME (Certain configurations)

Overview:
Windows XP ships by default with a **UPNP** (Universal Plug and Play) service which can be used to detect and integrate with **UPNP** aware devices. Windows ME does not ship by default with the **UPNP** service; however, some OEM versions do provide the **UPNP** service by default. Also, it is possible to install the Windows XP Internet Connection Sharing on top of Windows 98, therefore making it vulnerable.

As described on **upnp**.org: "**UPNP** architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. **UPNP** architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between".

Technical Details:
We at eEye believe that there are several security issues with the **UPNP** protocol itself; however, these more generic issues are out of the scope of this advisory. Expect a detailed paper to be released from eEye within the coming weeks.

This advisory covers three vulnerabilities within Microsoft's **UPNP** implementation. A remotely exploitable buffer overflow to gain SYSTEM level access to any default installation of Windows XP, a Denial-of-Service (DoS) attack, and a Distributed Denial-of-Service (DDoS) attack.

1. The SYSTEM Remote Exploit

The first vulnerability within Microsoft's implementation of the **UPNP** protocol can result in an attacker gaining remote SYSTEM level access to any default installation of Windows XP. SYSTEM is the highest level of access within Windows XP.

During testing of the **UPNP** service, we discovered that by sending malformed advertisements at various speeds we could cause access violations on the target machine. Most of these violations were due to pointers being overwritten. The following describes one instance of our testing:

Example Session:

NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CACHE-CONTROL: max-age=10
LOCATION: http://IPADDRESS:PORT/.xml
NT: urn:schemas-**upnp**-org:device:InternetGatewayDevice:1
NTS: **ssdp**:alive
SERVER: EEYE/2001 **UPnP**/1.0 product/1.1
USN: uuid:EEYE

If a buffer is incremented in the protocol, port, and uri fields of the Location URL and send sessions with 10,000 microsecond intervals, access violations will begin to be observed. In one situation, The EAX and ECX registers will contain addresses that are pulled from the memory that was overwritten and the svchost.exe process will access an invalid memory address at a "mov" instruction. It throws an access violation due to the fact that the destination address is an overwritten pointer, but there is nothing interesting at 0x41414141.

During our testing we discovered that there are multiple points of exploitation. We found instances of stack overflows and heap overflows, both of which were exploitable. In the case of the heap overflow we saw pointers being overwritten for both buffers and functions.

The **SSDP** service also listens on Multicast and Broadcast addresses. Therefore gaining SYSTEM access to an entire network of XP machines is possible with only one anonymous UDP **SSDP** attack session.

2. The DoS and DDoS

UPNP consists of multiple protocols, one of which being the Simple Service Discovery Protocol (**SSDP**). When a **UPNP** enabled device is installed on a network, whether it be a computer, network device, or even a household appliance, the device sends out an advertisement to notify control points of its existence. On a default XP installation, no support is added for device control as it would be the case in an installation of **UPNP** from "Network Services".

Although Microsoft added default support for an "InternetGatewayDevice", if an application is set up to "sniff" a network with XP, XP can be observed searching for this device as XP is loading. This support was added to aid leading network hardware manufactures in making **UPnP** enabled "gateway devices".

By sending a malicious spoofed UDP packet containing an **SSDP** advertisement, an attacker can force the XP/ME client to connect back to a specified IP address and pass on a specified HTTP/HTTPS request.

An example session:

NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CACHE-CONTROL: max-age=1
LOCATION: URL
NT: urn: schemas-**upnp**-org:device:InternetGatewayDevice:1
NTS: **ssdp**:alive
SERVER: EEYE/2001 **UPnP**/1.0 PASSITON/1.1
USN: uuid:EEYE

The above packet data needs to be sent as a UDP packet to port 1900 of the XP/ME machine.

When the XP machine receives this request, it will interpret the URL following the LOCATION header entity. With no sanitizing of the URL it is passed on to the functions in the Windows Internet Services API. The string is broken down and the new session is created.

For example:
LOCATION: http://xptest.example.com:19/himom.html

A malicious attacker could specify a chargen service on a remote machine causing the XP client to connect and get caught in a tight read/malloc loop. Doing this will throw the machine into an unstable state where CPU utilization is at %100 and memory is being allocated to the point that it is totally consumed. This basically makes the remote XP system completely unusable and requires a physical power-off shutdown.

Attackers could also use this exploit to control other XP machines, forcing such machines to perform Unicode attacks, double decode, or random CGI exploiting. Due to the insecure nature of UDP, an attacker can exploit security holes on a web server using **UPNP** with almost total anonymity.

One of the bigger problems, and why this can become a DDoS attack, is that this **SSDP** announcement can be sent to broadcast addresses and multicast. It is therefore possible to send one UDP packet causing all XP machines on the target network to be navigated to the URL of choice, performing an attack of choice.

Also since parts of the **UPNP** service are implemented as UDP (in our opinion, a bad idea), it makes all of these attacks completely untraceable.

Vendor Status:
Microsoft has released a patch and security bulletin which is located at:

http://www.microsoft.com/technet/security/bulletin/MS01-059.asp

To verify that the patch has been installed on your system, do the following:

Windows 98 and 98SE:
Select Start, then Run, then run the QFECheck utility. If the patch is installed, "Windows 98 Q314941 Update" will be listed among the installed patches. To verify the individual files, use the file manifest provided in Knowledge Base article Q314941.

Windows ME:
Select Start, then Run, then run the QFECheck utility. If the patch is installed, "Windows Millennium Edition Q314757 Update" will be listed among the installed patches. To verify the individual files, use the file manifest provided in Knowledge Base article Q314757.

Windows XP:
Confirm that the following registry key has been created on the machine: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP1\Q315000. To verify the individual files, use the date/time and version information provided in the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP1\Q315000\Filelist.

The Common Vulnerabilities and Exposures (CVE) project has assigned the following two IDs:
The Buffer Overflow: CAN-2001-0876
The Denial of Service: CAN-2001-0877
This is a candidate for inclusion in the CVE list http://cve.mitre.org) which standardizes names for security problems.

We would strongly suggest denying all **UPNP** traffic at your internet borders as there is really no need to allow **UPNP** traffic across the Internet. Also, it would be wise to completely turn off the **UPNP** services as most users are probably not utilizing them. The less services running on your machine, the safer you will be. The **SSDP** Discovery Service and Universal Plug and Play Host service should both be set to disabled.

Credit:
Discovery: Riley Hassell

With extra help from:
Ryan Permeh - for technical advice and exploitation analysis for those difficult reverse engineering situations that Ryan has wet dreams about.

Marc Maiffret - as always with superb technical insight helping to discover and exploit the vulnerabilities in this advisory and once again proving that two heads are better than one.

Neothoth - "The typing machine", for camping out day and night in the eEye lab hammering vulnerabilities in URL handlers. Neo rocks :)

Related Links:
http://www.microsoft.com/technet/security/bulletin/MS01-059.asp

Greetings:
Mr. Patron and his tequila and the Three Wise Men (Jim, Jack and Johnny). Also Abraxas coffeeshop in Amsterdam.
eEye would like to offer thanks to all organizations supporting full disclosure, especially Securityfocus.com and NMRC. Don't let silly politics get in the way of what is right for everyone's security.

Oh yeah, one more thing:

Four score and numerous advisories ago, a security company set off to tell the world about its love of Tequila. However, little did people know, the team was not even legal. Now that the youngins Marc and Riley turned 21 this November we are all officially legal. That means the next time the NSA buys us beer at a SEC conference, they won't be breaking the law.